Abstract

There is provided a configuration enabling prevention in advance of leakage and outflow of secret information in the local network, such as private data and content whose copyright and use right is restricted. A plurality of identification information of a communication destination device are acquired at different data processing levels. Identification information acquired by data processing at a level of a physical layer or a data link layer of the OSI reference model and identification information acquired by data processing at a layer level of a network layer or higher are received and these identification information are matched. In addition, at least one of identification information receives generated data generated by an encryption process or a hash value generation process based on secret information shared with the communication source device. By matching a plurality of identification information and in accordance with a satisfied or an unsatisfied state of the matching, it is determined whether or not the communication destination device is a device connected to the same local network.